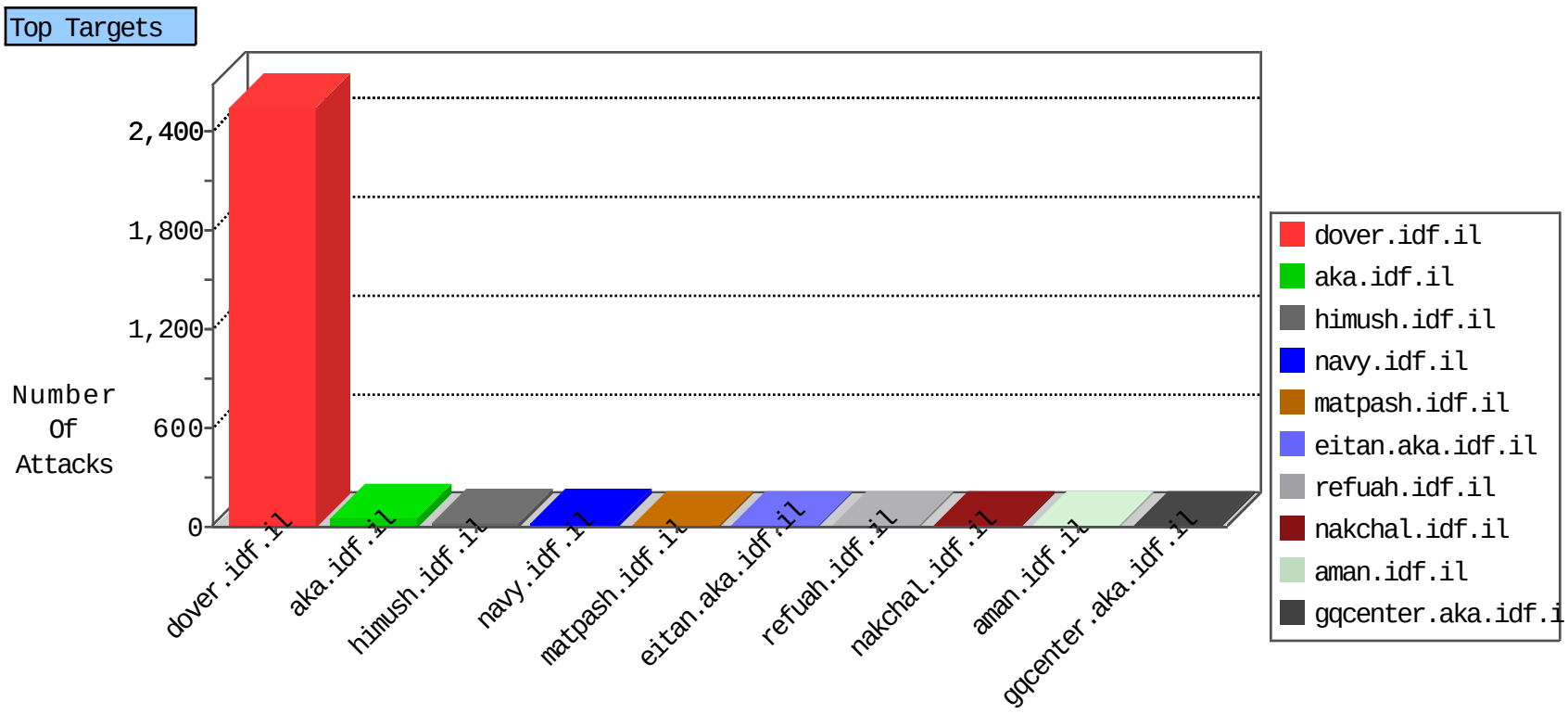
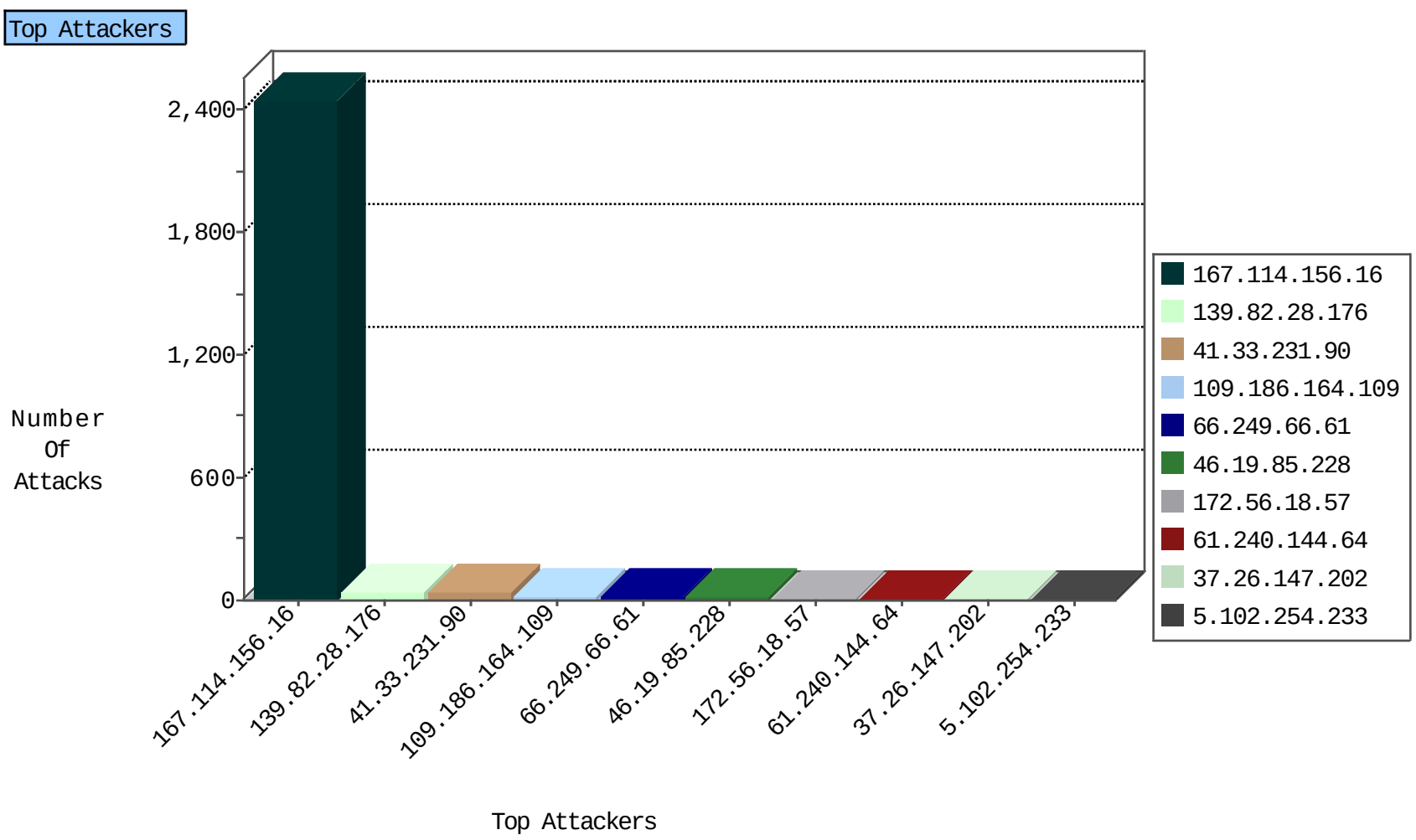
12-02-2015-02:04:00 to 12-02-2015-03:04:00

IDF Under Attack Daily Report





12-02-2015-02:04:00 to 12-02-2015-03:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3314
66.249.66.5	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	23
93.174.93.151	Netherlands	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1
93.174.93.151	Netherlands	147.237.76.176	test.ncore.idf.i	Block_Udp_All_Nets	drop	1

12-02-2015-02:04:00 to 12-02-2015-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.152.87	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
69.30.215.130	United States	147.237.77.226	www.chamatz.aka.idf.il	C1000106: HTTP: majestic bot	Block	1
159.253.145.150	United States	147.237.72.166	aka.idf.il	C095: Suspicious Addresses MFA	Permit	1

12-02-2015-02:04:00 to 12-02-2015-03:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.5	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
97.105.43.174	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.252.84	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.64	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
182.72.242.152	147.237.0.33	India	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
182.72.242.152	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
180.153.104.125	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.64	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
180.153.104.125	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -f -sS	1
24.121.225.29	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
149.202.186.50	147.237.76.199	Germany	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
204.13.204.139	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 2048	1
5.15.195.88	147.237.76.34	Romania	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.218.146	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
204.13.204.139	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -f -sS	1
89.248.172.140	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
183.60.252.84	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
182.72.242.152	147.237.0.35	India	akaws.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
182.72.242.152	147.237.0.19	India	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
182.72.242.152	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
180.153.104.125	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
149.202.186.50	147.237.76.201	Germany	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.15.195.88	147.237.76.34	Romania	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
209.126.116.147	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
149.202.186.50	147.237.76.197	Germany	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
204.13.204.139	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1

12-02-2015-02:04:00 to 12-02-2015-03:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.228	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
109.186.164.109	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
172.56.18.57	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
5.102.254.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.30.24.194	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
50.29.117.219	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.147.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.188.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.202	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.50	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
199.30.24.37	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.178.125.184	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
47.62.36.213	Spain	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
176.109.188.49	Ukraine	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
207.46.13.91	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
50.29.117.219	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
50.178.125.184	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
176.12.145.90	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.85.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.121.191	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.82.28.176	Brazil	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
64.125.239.183	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
149.88.110.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.121.180	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.186.164.109	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
176.12.145.90	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.85.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.162	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.22.134.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.82.28.176	Brazil	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
64.125.239.194	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
199.203.170.158	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.181	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.186.164.109	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
64.125.239.81	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.163	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
139.82.28.176	Brazil	147.237.77.234	halag.idf.il	drop	SAM rule	drop	1
37.26.149.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.189	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
64.125.239.151	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.3.144.162	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.163	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
139.162.218.146	Netherlands	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
139.82.28.176	Brazil	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 139.82.28.176	Block	8
139.82.28.176	Brazil	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 139.82.28.176	Block	4
207.46.13.56	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
139.82.28.176	Brazil	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 139.82.28.176	Block	4
139.82.28.176	Brazil	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 139.82.28.176	Block	4
139.82.28.176	Brazil	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 139.82.28.176	Block	4
139.82.28.176	Brazil	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 139.82.28.176	Block	3
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
2.54.151.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.167.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
139.82.28.176	Brazil	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	2
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Suspicious Response Code_Custom_Temporary	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
150.70.173.10	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20422-he/idfgdover.aspx	Block	1
139.82.28.176	Brazil	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
139.82.28.176	Brazil	147.237.76.30	himush.idf.il	Distributed PHP Attempt	Block	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
157.55.39.76	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/lite/contentsecurity	Block	1
139.162.218.146	Netherlands	147.237.76.30	himush.idf.il	Unauthorized Method OPTIONS for /	Block	1
64.39.109.20	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
79.180.125.178	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
157.55.39.17	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.17	Block	1
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
139.82.28.176	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/library/generaldoc.asp	Block	1
190.58.249.4	Trinidad and Tobago	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
150.70.173.8	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
64.39.109.20	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
207.46.13.91	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.144.62.184	Netherlands	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
157.55.39.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
23.254.113.26	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
139.82.28.176	Brazil	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
139.82.28.176	Brazil	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
212.227.29.47	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.67.243	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/list.asp	Block	1
190.58.249.4	Trinidad and Tobago	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
150.70.173.8	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/111177.pdf	Block	1
207.46.13.95	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1
85.144.62.184	Netherlands	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
157.55.39.17	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1